TOO GOOD TO BE TRUE….

A Column on Consumer Issues
by Attorney General Wayne Stenehjem's
Consumer Protection and Antitrust Division

September 17, 2003

Preventing Identity Theft – Consumer Quiz.

Identity theft is on the rise across the nation. If your wallet is stolen, you know what to do. But how do you protect yourself from other, less obvious, attempts to steal your money and identity? Try this CONSUMER QUIZ and find out!

1. Identity theft is:
    a. Switching places with your identical twin;
    b. Using key pieces of someone else's personal identifying information in order to impersonate them and commit various crimes in that person's name;
    c. The newest Nintendo™ game.

Answer: b. In addition to basic information like name, address, and telephone number, identity thieves look for social security numbers, driver's license numbers, credit card and bank account numbers, as well as bank cards, telephone calling cards, birth certificates or passports. This information enables the identity thief to commit numerous forms of fraud.

2. Shoulder surfing is:
    a. A new type of surfboard;
    b. When someone looks over your shoulder to learn your password or PIN number;
    c. A high school sporting activity.

Answer: b. Criminals acquire account information while hanging out in banks and ATM lines, or at airports to get calling card number and information that they later sell to others. They get the money, and the victim gets the bill.

3. Dumpster Diving is:
    a. A new water sport;
    b. Thieves scavenging for documents in commercial or residential dumpsters;
    c. The official term for a belly flop.

Answer: b. Thieves look through the trash for canceled checks, bank statements, pre-approved credit cards, etc. They then use this information to steal your identity. Protect yourself by shredding or tearing up your canceled checks, statements, and any pre-approved credit card offers and other similar junk mail.

4. A skimmer is:
    a. A net used when crabbing;
    b. An electronic device used by criminals;
    c. The new Honda SUV.

Answer: b. A skimmer is an electronic device used by criminals to "swipe" your credit card without your knowledge and store information that enables them to use your account. The machine copies information from the card's magnetic strip, and the thief then creates a counterfeit card with the same account data. As the counterfeit card is a copy of your card, the thief has instant access to your account and can withdraw money or charge items just as you can. One skimming device alone can hold information from more than 200 accounts. At an average loss of $3,100 per card, a single device can wreak havoc. Magnetic stripe readers are openly sold on the Web because they have legitimate purposes, such as at trade shows and hotels.

5. Opt-out is:
    a. Not joining your colleagues for a drink after work;
    b. A good way to restrict your financial institutions from sharing your personal information;
    c. A new take-out restaurant.

Answer: b. Federal law requires banks, credit card companies, brokerage firms and insurance companies to send you a "privacy notice" each year – including a toll-free number or form to prohibit them from selling your data to unaffiliated "third-party" companies. If you choose to deny the company the right to sell your data to other companies, you are exercising your right to "opt-out." You may "opt-out" at any time. You may also ask your financial institution not to disclose information to its own affiliated companies. And you can tell other businesses you want to opt out of them sharing your information – from your telephone or cable company to charities, stores, catalog companies and web sites.

6. The "Do Not Call" list is:
    a. The best way to stop your daughter's boyfriends from calling;
    b. A telemarketer's nightmare;
    c. A list of stores you don't want to shop in again.

Answer: b North Dakota "Do Not Call" laws took effect on August 1, 2003. Consumers can register home and cell phone numbers at www.ag.state.nd.us or toll-free at 1-888-382-1222. Telemarketers cannot call the numbers registered on the list. Telemarketers must update their call lists at least every 90 days to remove registered numbers. If you receive a telemarketing call more than 90 days after you registered on the "Do Not Call" list, you can contact the Attorney General's Consumer Protection Division to report the violation. You will need to know the date and time of the call, the name of the company and, if possible, the name of the person who placed the call. Even if you are not on the list, telemarketers cannot use pre-recorded messages (unless a live operator first obtains your express permission) or block your caller-ID.

7. A “Sniffer” is:
    a. A dog;
    b. A software program;
    c. A cold.

Answer: b. A “sniffer” is a software program designed to “sniff out” and capture your financial data, passwords, addresses or other personal information being sent over networks. It is usually hidden in an e-mail attachment and activates secretly when you open the e-mail, sending the information back to the hacker without your knowledge. The best prevention is not to open e-mails from people whose names you don’t recognize – and regularly scan your computer with a virus detection program.

8. “Phishing” (pronounced fishing) is:
    a. A card game;
    b. A new type of e-mail scam;
    c. A medieval jousting event.

Answer: b. “Phishing” (also called “carding”) is a high-tech e-mail scam to deceive consumers into disclosing their credit-card numbers, bank-account information, social security numbers, passwords, and other sensitive information. The consumer receives an e-mail that claims to be from businesses the potential victim deals with – such as their Internet service provider, online payment service or bank. The fraudsters tell the consumers they need to “update” or “validate” their billing information to keep their accounts active, and direct them to a “look-alike” website of the legitimate business, further tricking consumers into thinking they are responding to a bona fide request. Unknowingly, consumers submit their financial information – not to the businesses – but to the scammers, who use it to order goods and services and obtain credit. The consumer has just become a victim of identity theft. If you receive an e-mail warning you that an account will be closed unless you reconfirm your billing information, do not respond or click on the link in the e-mail. Instead, contact the company cited in the e-mail using its regular business phone number.

Those are a few of the most common identity theft scams. A few simple precautions can protect you from the devastating consequences of identity theft. You can find more information, including tips on protecting your identity at www.ag.state.nd.us or http://www.consumer.gov/idtheft/.

The Attorney General’s Consumer Protection Division investigates allegations of fraud in the marketplace. Investigators also mediate individual complaints against businesses. If you have a consumer problem or question, call the Consumer Protection Division at 328-3404, toll-free at 1-800-472-2600, or 1-800-366-6888 (w/TTY). This article and other consumer information is located on our website at www.ag.state.nd.us.

* * * * *